

## Connecting the dots

### U.S. Army forges national intelligence support for troops in Iraq

By Glenn W. Goodman Jr.  
March 01, 2005

The challenges of the insurgency in Iraq have driven a number of U.S. Army initiatives designed to improve intelligence capabilities for its soldiers while making fundamental changes in the way the Army's military intelligence personnel do business. As Lt. Gen. Keith B. Alexander, deputy chief of staff of the Army for intelligence (G-2), frequently says: "Army intelligence is transforming while at war."

The focus is on increasing intelligence collection at the tactical level and supplying "actionable" intelligence — timely and useful information on the enemy and environment — to those closest to the fight. Two other key thrusts are improving the support of tactical units by national intelligence agencies through better access to national databases and analytical capabilities, and speeding analysis of the large volumes of collected data using advanced software tools to "connect the dots" and help generate actionable intelligence.

"In Operation Iraqi Freedom, we were once again confronted with the paradox that the soldier out front has the best tactical view of the battlefield but the poorest access to the specialized intelligence information available to national-level analysts. On the other hand, the national-level analyst has the best specialized information about enemy activities but the poorest view of the battlefield," Alexander said. "Actionable intelligence, with its emphasis on better collection, reporting and linked analytical efforts, directly addresses this paradox."

Actionable intelligence, one of 17 focus areas created in 2003 by Army Chief of Staff Gen. Peter Schoomaker, is defined as that which "provides commanders and soldiers a high level of shared situational understanding, delivered with the speed, accuracy and timeliness necessary [for them] to operate at their highest potential and conduct successful operations."

The Army's operations in Iraq have been far more decentralized than those of the recent past. With no rear areas or safe havens, Army soldiers and Marines have wrestled with instability and sought to blunt incessant attacks on U.S. and Iraqi forces from the shadows by insurgents who use small arms, improvised explosive devices and suicide bombs.

The Army soon recognized that all of its soldiers — down to dismounted troops at the lowest tactical level — needed to become intelligence collectors.

"The threat is all around us," Alexander said. "That requires us to go from what predominantly would have been signals intelligence and imagery intelligence systems to human intelligence. And the most prolific sensor in that regard is every soldier we have out on the battlefield."

As an Army document states, "Just as all soldiers must be prepared to fight as infantry, they also must serve as intelligence collectors. In Iraq and Afghanistan, soldiers are immersed in a dynamic operating environment. Every day, in the towns, cities and countryside, soldiers talk to inhabitants and observe more relevant information than all our combined technical intelligence sensors can collect. Soldiers also differ from other collection systems in that they interact with the populace. Clearly, soldiers are exposed to information that would be of significant value if collected, processed and integrated into a Common Operating Picture."

In August 2003, an Army survey team went to Iraq and assessed intelligence needs there. Collin Agee, director of ISR integration in the Army's G-2 office, said that one of the things the team found was that an estimated 400,000 patrols had been conducted throughout Iraq over three months, but only about 6,000 reports had made it up to brigade level.

"We must transform operational units to take an active role in pursuing intelligence," Alexander said. "Patrolling units must take the initiative to collect intelligence. ... The battalion carries out 50 to 100 patrols a day. They sweep up a lot of information that may be important. We lose a lot of that information today [because it requires] writing out a report."

One solution that the Army came up with was to begin fielding a small, hand-held personal digital assistant (PDA) device late last year in Iraq that makes reporting quick and simple. The Army planned to field the devices in Afghanistan early this year. Called the Force XXI Battle Command Brigade and Below-Commander's Digital Assistant (FBCB2-CDA), it allows soldiers to digitize reports "at the point of origin." The reports are passed to an operations center, where they are consolidated and then passed back down to all the CDAs and FBCB2 vehicle-mounted systems in the area of interest.

The device uses a satellite-based network to receive and transmit data and can display text fields as well as a map with icons representing friendly and enemy locations. Situational awareness updates are transmitted over the network every five minutes. If a patrol spots a sniper and reports it, other small units are alerted and can help target the sniper or avoid the area.

"Just because there were only 6,000 reports out of 400,000 patrols doesn't mean that there were no [paper] reports written. There were. But they didn't go anywhere. They didn't get into digits, so those reports were stopped at battalion level, which filtered out what they thought might be of interest to brigade level. And then, with gross latency, that information would then go to higher echelons," said Maj. Gen. John Kimmons, commanding general of the U.S. Army Intelligence and Security Command at Fort Belvoir, Va. "So it was a series of filters, with everyone trying to do the right thing, which constrained the flow of information so that we missed a lot that was relevant."

If an Army patrol in Iraq kills a sniper, for example, it's important that the patrol report the incident and location rather than just move on, Kimmons said, because the fact that a sniper was encountered in a particular neighborhood becomes part of a larger pattern over time that could identify a hot spot of enemy activity.

"If they don't report the sniper, then we don't capture that data," he said. "That is what the PDA solutions are principally designed to solve, which is to proliferate a really simple way for soldiers without much training to report the essential elements of enemy activity and also situational information into digits to get them into a data base. The report isn't filtered by anybody, and the same information is rapidly shared at different levels."

The Army's initial goal is to field 1,000 of the PDAs and to get them into the hands of its soldiers in Iraq and Afghanistan as quickly as possible. Army tactical human intelligence, or humint, teams and combat patrols are being given the devices first. Feedback from the troops in the field will be used to refine the design of the devices.

Other steps being taken by the Army to improve intelligence collection at the tactical level, Agee said, are widely dispersing unmanned aerial vehicles among its military intelligence units and doubling the number of human intelligence and counterintelligence personnel.

"We will have humint teams down at the brigade level. So at that low tactical level, the commander will have a humint capability at his disposal that he can send into towns and villages," he said.

#### **TACTICAL OVERWATCH**

Another major Army intelligence initiative designed to support its combat troops is called Tactical Overwatch. Alexander said it involves focusing "analytical efforts at higher echelons in

direct support of designated tactical forces at the supported units' level of granularity. Operating from fixed sites, overwatching elements will exploit the shared knowledge of the entire network, with access to forward area and national collection, shared databases and advanced processing, enhancing situational awareness for overwatched units, particularly when they are actively engaged or moving."

Each Tactical Overwatch team of 15 to 20 dedicated personnel, including experts in human, signals and imagery intelligence, will function as a mini-intelligence analysis center. It will operate around the clock as it supports a brigade in the field with up-to-date, all-source intelligence tailored to planned missions in specific maneuver areas, such as a small sector of Baghdad.

"This is potentially our most important initiative in trying to serve our tactical customers," Agee said. "The overwatch team's computer screens and their collection and analysis will be focused on that small, finite area. So their heads are completely in the game, and in the United States are on the same cycle as the guys in the box. They are in the fight and prepared to provide better support than we can do now."

The new concept is having a trial run with the 3rd Infantry Division in Iraq this year, with Tactical Overwatch support coming from Intelligence and Security Command's Information Dominance Center at Fort Belvoir. Similar overwatch teams will exist within the command's five theater intelligence brigades by 2007 in support of brigade-level combat units (to be called "units of action" in the future) employed by Army component commanders. The overwatch teams will consist of uniformed, civilian and contractor personnel.

#### **FUSING ALL-SOURCE INTELLIGENCE**

"While we always need more and better access to sources of information in support of answering the hard questions for the war fighters, the heart of our intelligence challenge is not collection. It's to fully leverage intelligence that we've already collected," said Kimmons, who served as U.S. Central Command's director of intelligence for several years before taking over the Army's Intelligence and Security Command.

Agee agreed that intelligence exploitation, not data collection, is the challenge.

"During the Cold War, the challenge for us largely was collection. That's not the problem anymore. We've got incredible collection assets," he said. "You could say that we are drowning in data but starving for intelligence."

Intelligence and Security Command performs some intelligence collection and processing, but its primary role is analysis and fusion of intelligence data from around the globe as part of the joint Defense Department intelligence team. Yet, as Kimmons said, "Our analysts spend far too much time assembling and organizing data, as opposed to fusing it and analyzing it, to understand where it's leading. Moreover, most of our analysts are working with fractions of all the data that's already collected and reported.

"So how do they quickly integrate the latest ambiguous bits and pieces within the broader context of all the intelligence there is, for better, more complete understanding? Rapid all-source fusion analysis is what we are after. An intel question posed one time, and rubbed against the national, theater and tactical holdings that we already have to place it in a better context. And that requires information and database sharing, data structuring and the use of advanced software tools."

The Information Dominance Center, which has gained unusual access to national intelligence data through hard-fought agreements with intelligence agencies such as the National Security Agency, is pioneering the use of such intelligence exploitation tools. The tools are needed,

Alexander said, to “rapidly establish threat association and linkages, recognize threshold events, activity patterns and anomalies, understanding the significance of information ‘buried’ within large volumes of collected material.”

One such commercial software tool being adopted by the Information Dominance Center is called adaptable or dynamic signature graphs, which establish a baseline of normal behavior and sound an alert when thresholds are exceeded. Examples in the intelligence context might be when radios begin operating in areas where signals have never been transmitted before, when regular things stop happening, or when densities change or certain types of movements occur.

“If your credit card is being used for an odd transaction, Visa will call you anywhere in the world within four minutes,” Kimmons said. “Now, if they can do that with millions and millions of transactions and bits of data, then why can’t we harness that power in the software sense to let us rake across terabytes of data rapidly and find the little pieces, the changes, the anomalies, the kind of things that a brigade or battalion commander wants to know — that certain threat information has been reported by somebody, somewhere, sometime, or the confluence of reporting has come together to tell him in his sector of Baghdad that right now there is either an opportunity to do something or there’s a target or a threat or a danger? And do it at a classification level at which he can use it — the Secret level and even below that sometimes — even though the information may have come from a source at a much higher classification level.

“The answer is, we really can,” Kimmons added. “We’re pioneering it today within the Information Dominance Center. But there are some critical components. You’ve got to get near-real-time access to all of the collected data — all of the humint, signals intelligence and imagery intelligence — from the PDA of the squad on the street to things that are flying around above their heads, regardless of classification. You’ve got to structure the data in ways that let you rapidly search and visualize on your computer screen how the pieces interrelate and understand their significance and detect changes over time. Just like the cop in New York City does as he walks around his precinct and sees a new face or a new car and then talks to his informants.”

The Information Dominance Center, Kimmons said, has created “a network of databases at all levels of classification that we’ve tortuously engineered access to through a lot of agreements. Many of them are caveated and code-worded and originator-controlled. The idea is that by taking this interrelated series of databases, we can come a lot closer, using mostly commercial advanced software tools and techniques, to determining the significance, in a timely way, of collected pieces of intelligence.”

But the key is to provide more than access to data.

“Access to a lot of databases is good, but it’s also insufficient,” Kimmons said. “Even if all the databases that exist in the U.S. intelligence community — hundreds and hundreds — were all linked together somehow, you would not be able to fully leverage them or understand the significances that pertain to your particular area of interest unless you have a process to inject all that information and organize and structure it in a way that lends itself to visualization on a common geospatial [background]. Our capability is not at 100 percent, but it validates our ability to do it. What holds us back is not the technological difficulty; it’s the policy spider webs and reluctance to share intelligence at increasingly lower levels in near real time, where it is tactically relevant.” •